



安全与保密
2006年9月

防止内部攻击 :组织如何保护内部敏感信息

目录

- 2 简介
- 3 内部攻击威胁日益严重
- 5 您的组织正面临危险：
了解这种威胁的严重性
- 6 制定更加精密的安全措施
- 11 结束语

简介

现在，每年有大量业务交易通过电子方式进行，组织保存的敏感数据的数量不断增长。对于许多组织来说，数据已成为无价资产，是企业运营的命脉。越来越多的用户拥有访问这些数据的权限，其中包括员工、业务合作伙伴、供应商以及客户。IT 基础设施规模不断扩大、复杂程度日益提高、分布范围更广，而且更加便于访问。

这种互联性对企业、政府机构及消费者具有许多益处，但也同时带来极大风险。组织提供的访问点越多，危及系统安全或数据被盗的可能性就越大，其风险相当高，随着隐私信息库的扩大，这种情况变得更加严峻。企业和政府机构必须满足严格的监管规定，并保护其知识资产不受竞争对手及破坏性政治实体的侵害。而消费者最关注的是身份失窃以及其他隐私泄漏的潜在危险。

公众日益关切个人数据的安全性和隐私性，从而使许多企业和政府机构成为焦点。世界各国都在制定相应的监管措施，以维护信息的机密性。英国的法律近年来进一步完善，以防止欺诈和身份盗窃，如1998年颁布的“数据保护法”（Data Protection Act）。在美国，加利福尼亚州通过了“安全违反通告法”（Security Breach Notification Law），要求各企业（无论其所处地理位置）必须向加州市民通告数据欺诈事件。¹ 此后，另外23个州也通过了各自的通告法律。加拿大也计划采取类似的措施。新近的这些立法活动，以及频繁出现的有关安全侵犯事件的媒体报道，使人们明确地认识到这类威胁的确普遍存在。

要点

强有力的周边防御可以有效阻止外部威胁，但只能提供组织所需的部分保护。

尽管内部攻击威胁往往不像外部攻击那样引起足够重视，但内部威胁的确是每个组织面临的一个十分紧迫的问题。

IBM 在其2005年全球业务安全指数报告中指出，小规模、有针对性的攻击，而非蠕虫、垃圾邮件、病毒及其他恶意软件等席卷全球的威胁，正在成为一种新的发展动向。² 特别是，内部攻击会对数据安全和隐私构成严重威胁。本白皮书旨在使读者更好地了解内部攻击问题，并提供一些有助于组织规避内部攻击风险的建议。

内部攻击威胁日益严重

几十年来，各种组织力求实现两方面兼顾，既使用更加开放的分布式网络，又要采取更有力的措施防御各种入侵，包括采用防火墙、反病毒软件、生物特征识别和身份访问标记等。由于采取了这些措施，企业可以更加有效地防止来自外部的威胁，同时也使潜在黑客或病毒越来越难以侵入系统。不过，这些技术都属于被动方式，仅能阻止未经授权的访问。它们只是构成了第一道防线。

普华永道与 CIO 杂志公布的“2005全球信息安全状况”调查结果显示，33%危及信息安全的攻击源于内部员工，同时有28%来自前雇员以及过去的合作伙伴。³ 尽管企业界、政府机构和行业分析人士都承认内部安全侵犯构成的危险，但往往更多地关注那些更为突出的外部入侵，如拒绝服务攻击、广泛传播的病毒以及直接窃取知识或金融资产。

要点

“不诚实的内部人员”可以利用组织的漏洞进行身份欺诈，窃取保密信息，从而获得个人利益或作为团伙犯罪的一部分。

隐私权信息交流中心保存的一份清单显示，自2005年2月以来，仅美国报告的数据侵犯事件就达数百起。

然而，这种将外部威胁优先于内部危险加以防范的做法实际上误入歧途，会在组织防御体系中留下巨大隐患。2006年6月，后台处理及客户支持公司 HSBC Electronic Data Processing (India) Private 报告称，公司一名盗窃团伙的员工获取了客户借记卡信息，并利用这些信息骗取了英国20名客户425,000美元。⁴ 这起事件只是过去几年大量事件中的一例。美国隐私权信息交流中心保存的一份清单显示，自2005年2月发生轰动一时的 Choice-Point 数据侵犯事件以来，已发生了数百起此类事件。⁵ 许多此类事件都源于组织内部，该清单将其称之为“不诚实的内部人员”。请看以下几个隐私权信息交流中心清单中列出的例子：

- 一家综合证券公司的一名员工非法访问了100多条客户记录。
- 一家酒店的系统受到攻击，不是不诚实的内部人员所为，就是黑客作祟，造成55,000条记录汇漏，包括客户姓名、住址、信用卡细节、社会保险号码、驾照号码以及银行账户数据。
- “一名不诚实的内部人员，也可能是一个恶意软件”访问了一家网上支付公司的系统，窃取了用户的姓名、电话号码、住址、电子邮件地址、IP 地址、登录名和口令、信用卡类型及网上购物金额等数据。
- 一家保险公司的员工访问了保密数据，包括不可赎回财产数据中的姓名、社会保险号码、出生日期和地址等，并利用这些信息为自己牟取利益。

另有几个案例涉及笔记本电脑被盗、备份磁带丢失或未经授权设置或使用账户。⁵ 尽管严格来说这些事件未必都属于“内部攻击”，但它们却可以通过同样的方式给组织带来危险，利用经过授权的渠道绕过周边防御，从而避开检测。

要点

由于员工拥有合法授权，又熟知组织的漏洞，因此内部攻击比识别外部侵入企图更难以检测。

最近一项调查显示，骗局平均可维持18个月而不被识破。

未能识破的攻击可以造成严重后果，包括由于损坏数据而承担的法律 responsibility，丧失竞争地位及破坏业务运营等。

您的组织正面临危险：了解威胁的严重性

内部攻击有可能造成重大损失，其后果与外部攻击造成的损失相当，甚至更为严重。作为组织信任的一名成员，犯罪者拥有合法授权，并且可以相对自由地登入组织 IT 基础设施内部进行活动。这种攻击通常以特定信息为目标，并充分利用一些既有的入口点或潜在漏洞。从许多方面看，内部攻击比识别从外部侵入企图更难检测。

注册舞弊审核师协会在其“2006 ACFE Report to the Nation on Occupational Fraud and Abuse”报告中指出，诸如资产挪用、贪污或虚报报表等大多数普通舞弊案，都是由于偶然原因或通过员工提供的线索揭露出来的，这表明有效监测和监督极为不力。该报告还发现，骗局平均可维持18个月而不被识破。⁶

一直未被监测到的内部攻击会给组织造成重大损失。或许更为严重的是，这种攻击会泄漏客户或员工的信息。若发生此类行为，无论身份盗窃、数据滥用，还是出售敏感信息，都有可能使组织承担相关损失的法律 responsibility，并受到监管部门的处罚。此外，如果公司内部人员利用知识产权或商业秘密达到非法目的，还会使企业的竞争地位受到威胁。这种攻击的目的也可能是为了敲诈钱财或损害组织的声誉。如果攻击导致 IT 系统停机或受到破坏，还会妨碍业务运营并降低 IT 投资的价值。

既然危险如此之大，针对内部攻击的威胁采取相应措施，防患于未然已显得越来越重要了。

要点

分布式、全球化工作环境以及迅速变化的业务状况，要求组织全面兼顾最终用户访问能力与数据保护。

要防止内部攻击，安全系统需具备更高的精密度和粒度。

四种基本要素可使系统达到所需的精密度水平。

制定更加周密的安全措施

当前分布式环境以及迅速变化的业务状况（如并购、裁员和全球采购），使得用户地理位置分布的范围更加广泛，系统存在多个入口点，并且有可能导致员工产生不满。因此，当前的组织遭受内部攻击的风险更大。每个组织都应采取相应的策略，有效管理这种风险，全面兼顾最终用户的访问能力和安全防范。

监视内部攻击时（与外部攻击不同），检查是否安全的标准不再是“这一访问是否已获得授权？”而是“这一行为是否可以接受？”前一问题只是要求在某单一时间点上给出简单的“是”或“否”的答案，而后一问题面临的复杂性则要大得多。用户行为包括给定时间段内，由开始到结束发生的所有事件，涉及长时间的特征及微妙差异。要回答这一问题，要求系统具备更高的精密度和粒度。在后面的几页中，我们将介绍可作为解决内部攻击威胁整体防范措施的四个基本要素，以使系统达到所需的精密度水平，这四个基本要素分别是：行为分析、集成安全组件、自动响应以及迭代建模过程。

行为分析

阻止内部攻击的关键在于了解某一给定业务过程中正常行为的范围，并确定偏离常规的行为。因此，首要的步骤之一就是制定政策，即定义某一工作群体中可接受行为的参数。这些参数将成为比较分析的基线，因此基于历史数据或具体经验，而不仅仅是基于现实或不现实的业务预期

要点

安全系统应能自动监测授权用户的在线活动，检测出异常行为，甚至帮助阻止可能出现的误用行为。

行为分析有助于在高负荷的动态工作环境中，识别偏差和异常特征。

建立用户简档是十分重要的。（参数设置得过于宽松可能遗漏某些危险行为，导致这些行为无法被发现；而参数设置过于狭窄则有可能产生大量误报。）随着用户角色的转变，组织应相应更新简档文件。

既然采用参数作为比较分析的基线，安全系统就应该在每次会话中自始至终，自动监测授权用户的各种在线活动。系统不仅能够通过比较分析识别异常行为，而且还应预测甚至帮助预防潜在的误用，对某些触发事件做出及时响应。系统需要监测下列变量：

- 初始连接—登录日期及时间、相关的 IP 地址以及连接频率；
- 数据访问—数据请求，按照具体类型加以组织；
- 应用程序使用情况—使用频率及持续时间；
- 总体使用情况—总会话时间以及数据请求总量。

行为分析在高负荷的动态工作环境中是必不可少的，例如，在客户信息可能遭到欺诈或误用的呼叫中心。这些中心工作的员工有大量的机会访问客户记录，但他们在工作日访问的记录数量一般是能够预测的。例如，如果通过历史分析确定某一特定呼叫中心的每位工作人员通常每天访问10至15条记录，那么对访问30条甚至更多记录的工作人员，就有必要进行调查。同样，如果某位工作人员浏览通常对于客户交流来说并非必需的信息，那么就可以认为其形迹可疑。组织只有通过持续的、有对比的行为分析，才能识别这些异常行为。

要点

安全要素应彼此实时地无缝交互，从而使系统能够对潜在威胁进行透彻的分析并做出迅速响应。

有效的特征识别有赖于整个 IT 环境中不同监测系统消息和事件的关联。

集成安全组件

许多组织都至少拥有某些防范内部恶意攻击所需的基本安全要素，包括认证系统、资产追踪软件、设备及互联网使用情况的监测功能以及其他工具等。然而，这些要素彼此尽可能无缝协作是十分重要的。事实上，组织之所以感到检测内部攻击非常困难，原因之一就是花费大量时间分析来自各种设备、入口点以及用户账户的大量数据。

组织需要在某一粒度水平上实现各种安全组件之间的通信、关联和分析，这些组件包括认证网关、物理安全系统、资产管理工具、网络监测功能以及网络安全平台等。这些系统应该能进行实时通信，这样组织才能够迅速反应，防止数据被用于非法目的，甚至有可能预测并防止恶意攻击。

组织用来监测用户行为的系统在设计上，还必须简化管理员的监测及特征检测任务。管理员应能访问中央控制台，从网络设备到应用程序的使用，控制台汇集了系统监测的各种消息和事件。手动检查历史记录及跨系统搜索复杂的关系会占用太多精力，从而影响执行具有更高价值和优先级的活动。

如果各种事件在整个 IT 环境中被相互联系起来，我们可以设想组织的特征检测能力可以提高到何种程度。例如，某个组织可能运行一个通常不能远程访问的敏感程序。如果某位员工未通过标记阅读器或现场工作站等物理访问

要点

安全系统本身应该有能力对不可接受的用户行为做出即时响应。

自动拒绝访问可以阻止攻击的发生，并便于网络管理员采取适当的措施。

点登录该应用程序，那么集成系统就可以立即确定此行为异常，并有可能带来危害。没有这种自动实时关联功能，这一远程访问就可能无法被及时检测出来。即使几小时的延误都可能为潜在攻击者提供足够的作案机会。再举一个例子：一家信用卡呼叫中心可能在几周内记录了数条有关计费错误的顾客投诉。负责员工访问记录的管理员可以迅速检查同一时期内异常行为的特征。

自动响应

组织需要尽可能迅速地识别偏离常规的行为并做出响应。仅仅依靠人工检测及响应是不够的，尤其在攻击发生在非工作时间的情况下。

为预防或降低损失，系统本身应该能够对不可接受的行为做出及时响应。例如，一旦这种行为偏离标准的程度超出某一阈值，系统应拒绝对被请求的应用程序或数据库进行访问。这种近乎即时的响应便于网络管理员及时收到告警、分析行为特征并选择采取相应的措施。网络管理员也不必非得具备安全方面的高深专业知识，才能解释这种数据或决定后续行动步骤。安全系统应能基于安全威胁方面的最新研究和认识，自动给出一系列相关的响应建议。此外，系统应能对误报进行分类。仅仅传送信息，而不做基本分析的告警系统，对监测过程来说没有多大价值。

要点

面对不断升级的安全威胁，要想技高一筹，组织必须不断改进并提高安全防范能力。

自调整系统可在无人工干预的情况下，对动态的业务状况做出恰当的智能反应。

迭代建模过程

无论组织针对当前的安全威胁做出多么充分的准备，危险还是会不断升级。组织的员工不断流动；IT 基础设施会不断扩展并纳入新技术，而这些新技术可能会带来未曾预料到的漏洞。要保护敏感数据，组织必须不断努力，从而在应对潜在攻击方面技高一筹。在这种持续不断的努力中，安全系统应发挥重要作用。

重要的是，检测系统不能仅限于范围狭窄的具体规则，因为正当行为的范围会随着时间发生变化。实际上，组织应建立一种具有自调整能力的系统，这种系统能够对动态的业务状况做出恰当的智能反应，从而不必全面重新定义规则。例如，为达到某种成本或客户满意度指标，呼叫中心会频繁地更改呼叫的平均长度；或者，市场宣传活动可能要求工作人员访问通常并不需要的数据。如果对此类变化不具备动态调整能力，安全系统会向管理员发出大量误报，令其疲于应付，进而降低告警的价值。同时，系统需要设置阈值，这些阈值应足够敏感，以便从大量行为数据样本中检测出细微的偏离。只有通过迭代建模过程才能在以上两个极端条件之间达到一种平衡。在这个过程中，监测系统可以学习组织的正常步调，并对多种重叠层面的可接受行为进行分类。

要点

随着组织、合作伙伴、用户和顾客之间的界限逐渐模糊，组织必须做好准备，从源头上防御攻击。

结束语

最近发生的大量事件表明，各行各业的组织决不能对内部攻击的潜在威胁继续等闲视之。随着组织不断成长，其员工的地理分布越来越广，他们部署的系统异构程度、复杂性会不断提高，相互联系更加紧密，保存的机密数据越来越多，而所面临的监管要求也在不断发生变化。

现在组织、合作伙伴、用户和顾客之间的传统界限逐渐模糊，使得安全策略更加难以制定和实施。组织必须做好准备，从源头上防御攻击，针对传统企业与当前及未来开放的、分布式组织之间缺口中存在的漏洞，采取相应措施。

更多信息

作为安全和隐私服务领域的领先企业，IBM 全球服务部可帮助您更好地了解内部攻击的威胁，并思考如何采取可行措施加以解决。我们推出的IBM信息安全框架（Information Security Framework），旨在针对关键性安全问题，提供系统化的有效措施，从数据保护以及总体安全方面，帮助组织应对不断升级的威胁、危险以及业务需求。此外，IBM 企业优化中心（IBM Center for Business Optimization）可提供安全及隐私方面的独特见解，利用先进的数学研究、企业绩效管理、商业智能系统、软件以及深度计算，帮助组织制定有效策略。

欲了解更多信息，请与当地 IBM 销售代表联系，或发送电子邮件至：

IBM Center for Business Optimization

Toby Cook, Associate Partner, IBM Center for Business Optimization —
toby.cook@us.ibm.com.

IBM Information Security Framework

Michel Bobillier, Global Offering Executive, IBM Security and Privacy
Services — bobillier@ch.ibm.com

另请访问：

ibm.com/services



© IBM公司版权所有2006

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

美国印制

09-06

保留所有权利

IBM以及IBM标识为国际商业机器公司在美国及其他国家，或同时在美国和其他国家的商标或注册商标。

其他公司、产品和服务名称可能为其他公司的商标或服务标识。

本出版物提及的IBM产品或服务并不意味着IBM有意向IBM运营所在的所有国家提供这些产品或服务。

IBM对本文提供信息的准确性不承担任何责任，使用此类信息所带来的风险由信息接收者自行承担。本文信息如有变更或更新，恕不另行通知。IBM亦可能随时对本文所述产品和/或程序进行改进和/或更改，恕不另行通知。

-
- 1 California Security Breach Information Act (S.B. 1386) , 于2003年7月1日颁布 ; http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html
 - 2 IBM global business security index report, 2005.
 - 3 Scott Berinato (与 Research Editor Lorraine Cosgrove Ware共同编写) , "The Global State of Information Security 2005," 2005年9月15日 , 由 PricewaterhouseCoopers 和 CIO出版 ; <http://www.cio.com/archive/091505/global.html>
 - 4 "A Chronology of Data Breaches Reported Since the ChoicePoint Incident," Privacy Rights Clearinghouse ; 2006年8月5日由Privacy Rights Clearinghouse授权使用 ; www.privacyrights.org
 - 5 John Ribeiro, "HSBC claims customer fraud in Indian services center," Network World (IDG NewsService), 2006年6月27日 ; <http://www.networkworld.com/news/2006/062706-hsbc-claims-customer-fraud-in.html>
 - 6 "2006 ACFE Report to the Nation on Occupational Fraud and Abuse," Association of Certified Fraud Examiners; <http://www.acfe.com/fraud/report.asp>

GSW00316-USEN-00